

**Amendment and Response under 37 C.F.R. 1.116**

Applicant: Francisco Corella

Serial No.: 09/483,186

Filed: January 14, 2000

Docket No.: 10001559-1 (H300.126.101)

Title: LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATES

---

**REMARKS**

The following remarks are made in response to the Final Office Action mailed May 19, 2004. Claims 1-24 were rejected. With this Amendment and Response, claims 1, 9, 13, and 21 have been amended. Claims 1-24 remain pending in the application and are presented for reconsideration and allowance.

**Claim Rejections under 35 U.S.C. § 112**

The Examiner rejected claims 1-24 under 35 U.S.C. § 112, second paragraph stating "the terms "certificate authority" and "certificate" by definition, include a digital signature. The Examiner asserted that applicant has used both terms in conjunction with "unsigned certificate," which is opposite of the common use of "certificate authority" and "certificate."

Applicant respectfully submits that it is well settled that "[a] patentee is his own lexicographer." Canaan Prod., Inc. v. Edward Don & Co., 388 F.2d 540, 544; 156 USPQ 295, 298 (7th Cir. 1968). "A patentee can choose his own terms and use them as he wishes so long as he remains consistent in their use and makes their meaning reasonably clear." Ellipse Corp. v. Ford Motor Co., 452 F.2d 163, 167; 171 USPQ 513, 515 (7th Cir. 1971), cert. denied, 406 U.S. 948; 173 USPQ 705 (1972). "A patentee may define his own terms, regardless of common or technical meaning, and fairness to the patentee requires the court to accept his definition of words, phrases, and terms." Int'l Cork Co. v. New Process Cork Co., 6 F.2d 420, 422 (2d Cir. 1925).

The term "unsigned certificate" is clearly defined in amended independent claims 1 and 13 to be a certificate that associates a public key of the subject to long-term identification information related to the subject and is not signed by the certificate authority. Also, the term "certificate authority" is clearly defined in amended independent claims 1 and 13 as issuing unsigned certificates to a subject, the certificate authority maintaining a database of records representing issued unsigned certificates in which it stores a record representing the first unsigned certificate, wherein the issued unsigned certificates are valid until at least one of revoked by the certificate authority and expired. In view of the above, Applicant respectfully requests reconsideration and withdrawal of the 35 U.S.C. § 112 second paragraph rejection of claims 1-24.

**BEST AVAILABLE COPY**

**Claim Rejections under 35 U.S.C. § 102**

The Examiner rejected claims 1, 2, 6, 7, 8, 13, 14, 18, 19, and 20 under 35 U.S.C. § 102(e) as being anticipated by Andrews U.S. Patent No. 6,324,645.

The Andrews patent is directed to computer-implemented techniques based on digital certificates for managing the risks associated with a public key management infrastructure shared by multiple users. The digital certificates are issued and signed by a certificate authority. A security engine validates the user's digital certificate and controls use of the public key management infrastructure based on certain attributes of the digital certificate.

Applicant respectfully submits that the Andrews patent fails to teach or suggest every limitation in amended independent claims 1 and 13. For example, the Andrews patent does not teach or suggest unsigned certificates as recited in amended independent claims 1 and 13. Throughout the specification and claims of the Andrews patent, digital certificates are characterized as being signed by the issuing certificate authority (CA). For instance, the abstract of the Andrews patent discloses, "[t]he user (102) is associated (301) with a digital certificate (200) which is issued and digitally signed by a certification authority (CA)."

Amended independent claims 1 and 13 further include a limitation that the verifier maintains a hash table containing cryptographic hashes of valid unsigned certificates. Amended independent claims 1 and 13 are clarified to include issued unsigned certificates are valid until at least one of revoked by the certificate authority and expired. In contrast, the Andrews patent describes the use of hash functions as in generating a "message digest" by applying a hash function to a digital certificate prior to signing it, or as part of verifying the certificate. The Andrews patent also describes maintaining database records including "jurisdiction hashes" at the public key management infrastructure. A "jurisdiction hash" is defined in the Andrews patent beginning at col. 9, line 59, as a "one-way hash of the organization name." A jurisdiction hash is an embodiment of an "access label," which is a part of a digital certificate (see, e.g., reference number 216 in Figure 2). Consequently, the Andrews patent does not teach or suggest a verifier maintaining a hash table containing cryptographic hashes of valid unsigned certificates, as recited in amended independent claims 1 and 13.

In view of the above, Applicant respectfully submits that the Andrews patent does not teach or suggest every limitation in amended independent claims 1 and 13 and these independent claims are believed to be allowable. As dependent claims 2 and 6-8 further

**BEST AVAILABLE COPY**

**Amendment and Response under 37 C.F.R. 1.116**

Applicant: Francisco Corella

Serial No.: 09/483,186

Filed: January 14, 2000

Docket No.: 10001559-1 (H300.126.101)

Title: LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATES

---

define patentably distinct amended independent claim 1, and as dependent claims 14 and 18-20 further define patentably distinct amended independent claim 13, these dependent claims are also believed to be allowable. Therefore, Applicant respectfully requests reconsideration and withdrawal of the § 102 rejection to claims 1-2, 6-8, 13-14, and 18-20 and allowance of these claims.

**Claim Rejections under 35 U.S.C. § 103**

The Examiner rejected claims 3, 4, 15, and 16 under 35 U.S.C. § 103(a) as being unpatentable over Andrews U.S. Patent No. 6,324,645 in view of Maruyama U.S. Patent No. 6,393,563.

Claims 5 and 17 were rejected by the Examiner under 35 U.S.C. § 103(a) as being unpatentable over Andrews U.S. Patent No. 6,324,645 in view of Kausik U.S. Patent No. 6,263,446.

Claims 9 and 21 were rejected by the Examiner under 35 U.S.C. § 103(a) as being unpatentable over Andrews U.S. Patent No. 6,324,645 in view of Gasser U.S. Patent No. 5,224,163.

Claims 10, 11, 22, and 23 were rejected by the Examiner under 35 U.S.C. § 103(a) as being unpatentable over Andrews U.S. Patent No. 6,324,645 in view of Micali U.S. Patent No. 5,793,868 in view of Boyle 6,212,636.

Claims 12 and 24 were rejected by the Examiner under 35 U.S.C. § 103(a) as being unpatentable over Andrews U.S. Patent No. 6,324,645 in view of Micali U.S. Patent No. 5,793,868 in view of Boyle U.S. Patent No. 6,212,636 in view of Gasser U.S. Patent No. 5,224,163.

In view of the above, amended independent claims 1 and 13 are believed to be allowable. As dependent claims 3-5 and 9-12 further define patentably distinct amended independent claim 1; and as dependent claims 15-17 and 21-24 further define patentably distinct amended independent claim 13, these dependent claims are also believed to be allowable. Therefore, Applicant respectfully requests that the § 103 rejections to claims 3-5, 9-12, 15-17, and 21-24 be removed and that these claims allowed.

**CONCLUSION**

**BEST AVAILABLE COPY**

**Amendment and Response under 37 C.F.R. 1.116**

Applicant: Francisco Corella

Serial No.: 09/483,186

Filed: January 14, 2000

Docket No.: 10001559-1 (H300.126.101)

Title: LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATES

In view of the above, Applicant respectfully submits that pending claims 1-24 are in form for allowance. Therefore, reconsideration and withdrawal of the rejections and allowance of claims 1-24 is respectfully requested.

No fees are required under 37 C.F.R. 1.16(b)(c). However, if such fees are required, the Patent Office is hereby authorized to charge Deposit Account No. 08-2025.

Any inquiry regarding this Examiner Interview Summary and Amendment and Response should be directed to either William J. Streeter, Esq. at Telephone No. (970) 898-3886, Facsimile No. (970) 898-7247 or Patrick G. Billig at Telephone No. (612) 573-2003, Facsimile No. (612) 573-2005. In addition, all correspondence should continue to be directed to the following address:

**Hewlett-Packard Company**  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, Colorado 80527-2400

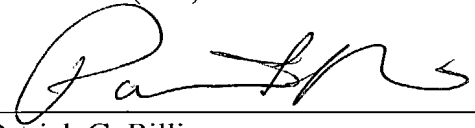
Respectfully submitted,

Francisco Corella,

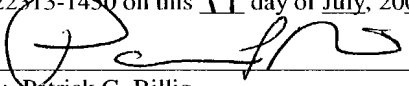
By his attorneys,

DICKE, BILLIG & CZAJA, PLLC  
Fifth Street Towers, Suite 2250  
100 South Fifth Street  
Minneapolis, MN 55402  
Telephone: (612) 573-2003  
Facsimile: (612) 573-2005

Date: July 19, 2004  
PGB: kle

  
Patrick G. Billig  
Reg. No. 38,080

**CERTIFICATE UNDER 37 C.F.R. 1.8:** The undersigned hereby certifies that this paper or papers, as described herein, are being deposited in the United States Postal Service, as first class mail, in an envelope address to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 19 day of July, 2004.

By   
Name: Patrick G. Billig

**BEST AVAILABLE COPY**